PROYECTAMOS SAS

MANUAL DE ROLES Y RESPONSABILIDADES DEL MODELO DE SEGUIRIDAD Y PRIVACIDAD DE LA INFORMACION "MSPI"



Proyectamos Colombia SAS

CONTENIDO

INTRODUCCIÓN 2
OBJETIVO 3
DEFINICIONES 4
ORGANIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) 5
COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 5
QUORÚM DEL COMITÉ 6
PARTICIPANTES Y RESPONSABILIDADES 6
CONTROL DE VERSIONES 9

INTRODUCCIÓN

La dirección de PROYECTAMOS SAS, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con sus clientes, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

El Desarrollo de este manual es basado en el Modelo de Seguridad de y Privacidad de la Información expuesto por el Ministerio de la Tecnologías de la Información y las comunicaciones, el cual recopila las mejores prácticas para suministrar requisitos para el diagnóstico, planificación, implementación, Gestión y mejoramiento continuo; lo anterior teniendo en cuenta las necesidades y objetivos, los requisitos de seguridad, los procesos misionales de PROYECTAMOS SAS.

OBJETIVO

Proponer la estructura de Gobierno de Seguridad que facilitará la emisión de políticas y el establecimiento de estándares, así como seguimiento al Sistema de Gestión de Seguridad de la Información que se aplicará en Proyectamos SAS.

DEFINICIONES

- Activo: Cualquier cosa que tenga valor para la organización. [ISO 27001:2005]
- Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. [ISO 27001:2005]
- Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. [ISO/IEC 27000: 2016]
- Incidente de seguridad de la información: Un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000: 2016]
- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas. [ISO/IEC 27000: 2016].
- SGSI: Sistema de Gestión de Seguridad de la Información.

ORGANIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Se establece la siguiente estructura institucional para el desarrollo, evaluación y mejora del SGSI:

COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Comunicar a los funcionarios, contratistas y/o partes interesadas que participan en actividades de forma directa o indirecta con la institución, la importancia de satisfacer los requisitos de seguridad y privacidad de la información.
- Establecer y modificar la política y los objetivos de seguridad de la información, orientados a la estrategia de la Institución, formulada en el plan estratégico, y los requisitos legales o contractuales
- Evaluar periódicamente el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI).
- Asegurar la disponibilidad de recursos necesarios para la implementación del SGSI.
- Priorizar proyectos o iniciativas de seguridad cuando se presenten riesgos o se perciba posibilidad de incumplimiento regulatorio.
- Definir, revisar y aprobar los objetivos de seguridad y los indicadores de SGSI.
- Aprobar la elaboración, modificación y anulación de documentos del SGSI.
- Aprobar los documentos y actualizaciones que se vayan generando como complemento al SGSI.
- Oficializar el documento "Declaración de Aplicabilidad", verificar su aplicación y soportar los proyectos de mejora que de esta declaración se deriven.

El Comité de Seguridad debe contar con miembros que tengan un amplio conocimiento de la institución, así como posición de liderazgo quienes ayuden a dinamizar el SGSI. El Comité de Seguridad hace parte del Comité Institucional de Gestión y Desempeño.

QUORUM DEL COMITÉ

El Comité de Seguridad de la Información sesionará con la participación de 3 de sus integrantes y decidirá con el voto favorable de la mitad más uno de los participantes. En caso de que la decisión del Comité presente empate se vuelve a llevar a una próxima reunión hasta que se logren los votos para la aprobación, dejando constancia en la respectiva acta.

PARTICIPANTES Y RESPONSABILIDADES

Se proponen

los siguientes integrantes del comité de seguridad de la información:

GERENTE TÉCNICO

El Gerente Técnico, debe apoyar activamente la seguridad de la información al interior de la Institución con un rumbo claro, alineado a los objetivos estratégicos. Este compromiso se verá reflejado a través de las siguientes responsabilidades:

- Creación de un Comité de Seguridad de la Información donde sea partícipe y se logre un mejoramiento continuo en la protección de los activos críticos, ciber activos e información sensible.
- Asignación de un responsable en seguridad de la información (líder o responsable de seguridad de la información).
- Aprobación del alcance, política, objetivos y políticas específicas de seguridad de la información.
- Realizar la revisión por la dirección del SGSI
- Asignar los recursos necesarios a los procesos para la implementación y mantenimiento del SGSI.
- Apoyar para que se cumpla con las políticas de seguridad de la información la interior de la Institución.
- Identificar y reportar riesgos, eventos o incidentes de seguridad a través de los canales definidos.
- Apoyar en la implantación de las mejorar identificadas en el SGSI.

LÍDER O RESPONSABLE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El líder o responsable de seguridad de la información tendrá las siguientes responsabilidades:

- Diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad privacidad de la información, y someterlos a decisión del Comité de Seguridad, realizando la implementación y seguimiento de los mismos.
- Coordinar la gestión de riegos de acuerdo con la periodicidad establecida, incluyendo la actualización de amenazas, vulnerabilidades y riesgos en los activos críticos, ciber activos e información sensible.
- Brindar lineamientos para controlar el acceso a los sistemas de información y la modificación de los privilegios.
- Vigilar el seguimiento a las no conformidades, el estado de las acciones correctivas, además de las quejas reclamos y sugerencias relacionadas con seguridad y privacidad de la información.
- Asegurar que se establecen, mantienen e implementan los procesos necesarios para el desarrollo del Sistema de gestión de seguridad de la información, SGSI.
- Presentar los informes del SGSI, incluyendo las principales novedades, iniciativas e incidentes de seguridad de la información, así como las lecciones aprendidas.
- Coordinar las reuniones del Comité de Seguridad de la Información y/o convocar a Comité extraordinario cuando las circunstancias o uno de sus miembros lo requieran, con motivo de riesgo mayor para la institución.
- Velar por el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información. Informar a la Alta Dirección sobre el desempeño del Sistema de Gestión de Seguridad de la Información y de cualquier necesidad de mejora.
- Estar en contacto con grupos especiales en temas de seguridad de la información, con el fin de estar documentado acerca de los nuevos métodos y herramientas de ataque
- Coordinar las actividades correspondientes a la gestión de Incidentes de Seguridad de la información.
- Desarrollar, mantener y comunicar las políticas, estándares y guías de seguridad de la información.
- Identificar y reportar riesgos, eventos o incidentes de seguridad a través de los canales definidos.
- Realizar el proceso de gestión de incidentes de seguridad que se presenten en la institución.
- Soportar a los líderes de proceso en el análisis de riesgos de seguridad y privacidad de la información y consolidar los planes de manejo de los mismos. Recibir capacitaciones en seguridad de la información.
- Recibir capacitaciones en seguridad de la información. • Elaborar las campañas de sensibilización, capacitación y socialización del SGSI.
- Coordinar junto con el líder de gestión de Recursos Tecnológicos:
- El fortalecimiento de la seguridad (hardening) de Servidores, Enrutadores y Switches involucrados en la red.
- La correcta configuración y efectividad de las herramientas de seguridad instaladas.

- La realización de pruebas de penetración y Ethical Hacking sobre la infraestructura de la institución.

LÍDER GESTIÓN DE RECURSOS TECNOLÓGICOS

El líder de gestión de Gestión de Recursos Tecnológicos en pro de garantizar el correcto uso y administración de los recursos informáticos de la institución y aseguramiento de la información debe:

- Actualizar el listado de activos de información, así como su valoración.
- Planear y ejecutar el plan de mantenimiento en los equipos de cómputo e infraestructura de la institución.
- Participar en la elaboración del cronograma de capacitación del SGSI en la institución.
- Implementar las mejorar identificadas en el SGSI que estén relacionado hardware, software, canales de comunicaciones de datos o infraestructura TI.
- Identificar y reportar riesgos, eventos o incidentes de seguridad a través de los canales definidos.
- Gestionar recursos para el SGSI.

LÍDER DE PROCESOS

Los líderes de procesos actúan como el "responsables de los activos de información" para todos los aspectos de seguridad de la información y tienen las siguientes responsabilidades:

- Identificar e inventariar los nuevos activos de información y los riesgos asociados.
- Verificar los informes de auditorías realizadas al SGSI y velar porque se apliquen las acciones correctivas identificadas, así como las recomendaciones entregadas por los auditores.
- Realizar el análisis de riesgos de seguridad de la información de sus procesos y coordinar el plan de manejo con el líder de seguridad.
- Determinar opciones de mejora en seguridad de la información en los procesos a cargo.

PROPIETARIO DEL ACTIVO

Es el funcionario que tiene bajo su custodia (o se le ha asignado) un activo. Sus responsabilidades son:

- Acompañamiento para la clasificación del activo de información
- Identificación de riesgos relacionados con el activo.
- Verificar el cumplimiento de la política de seguridad y privacidad de la información.
- Actualización permanente de la información del activo bajo su cargo.
- Implementar y cumplir con los controles relacionado con las funciones asignadas.
- Reporte inmediato de incidentes de seguridad de la información

CONTROL DE VERSIONES

Última revisión: junio 2023

Revisión: junio 2022

Revisión: junio 2021

- Creado en Julio 2020 por la gerencia técnica.